FIG. 1

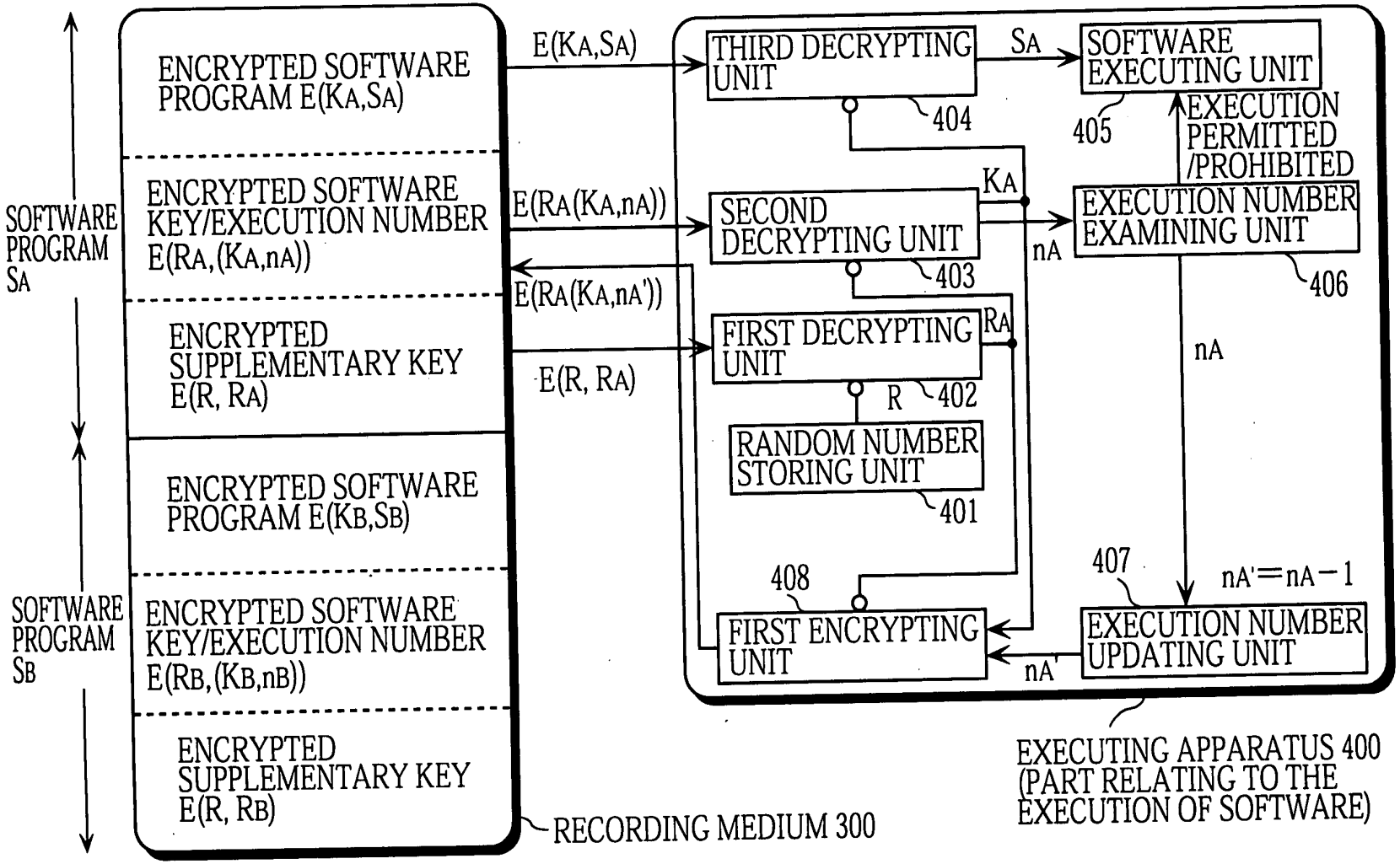

SOFTWARE PROGRAM SA
SOFTWARE PROGRAM SB
ENCRYPTED SOFTWARE PROGRAM E(KA,SA)
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER E(RA,(KA,nA))
ENCRYPTED SUPPLEMENTARY KEY E(R, RA)
ENCRYPTED SOFTWARE PROGRAM E(KB,SB)
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER E(RB,(KB,nB))
ENCRYPTED SUPPLEMENTARY KEY E(R, RB)
RECORDING MEDIUM 300
E(KA,SA)
E(RA(KA,nA))
E(RA(KA,nA'))
E(R, RA)
THIRD DECRYPTING UNIT
404
SA
SOFTWARE EXECUTING UNIT
405
EXECUTION PERMITTED /PROHIBITED
KA
SECOND DECRYPTING UNIT
403
nA
EXECUTION NUMBER EXAMINING UNIT
406
RA
FIRST DECRYPTING UNIT
R
402
RANDOM NUMBER STORING UNIT
401
nA
408
407
nA'=nA−1
FIRST ENCRYPTING UNIT
nA'
EXECUTION NUMBER UPDATING UNIT
EXECUTING APPARATUS 400 (PART RELATING TO THE EXECUTION OF SOFTWARE)

FIG. 2

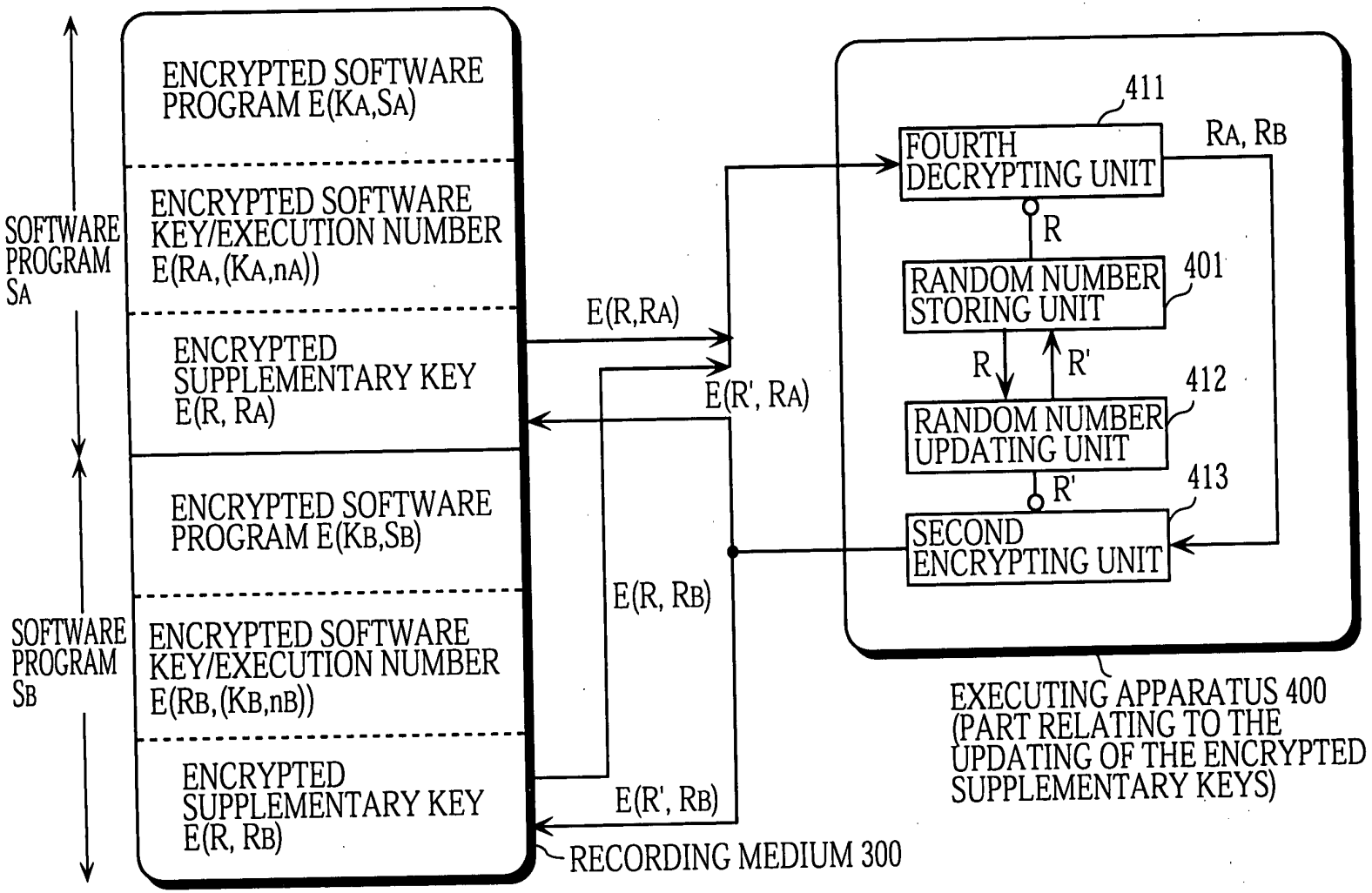
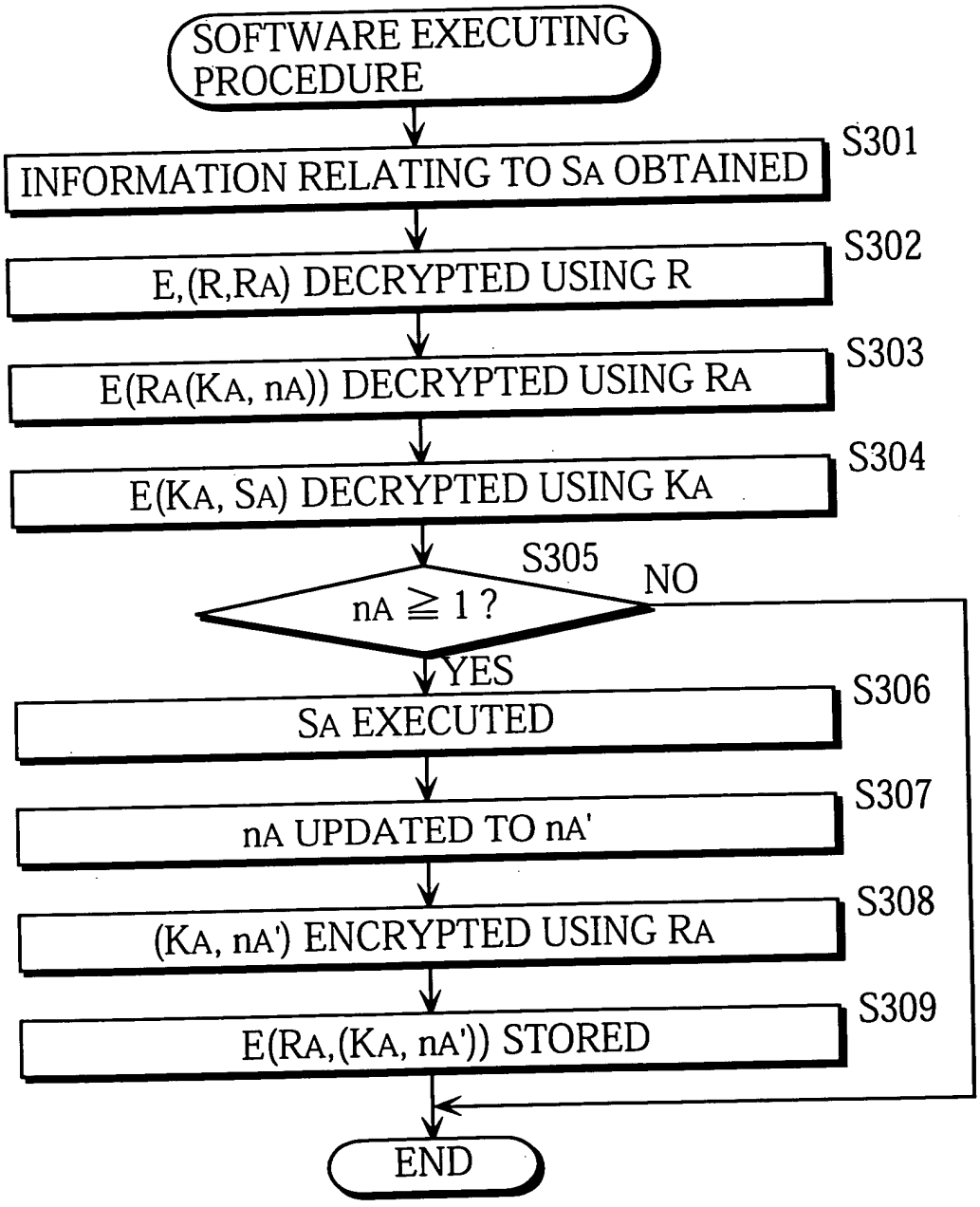

ENCRYPTED SOFTWARE PROGRAM E(KA,SA)
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER E(RA,(KA,nA))
ENCRYPTED SUPPLEMENTARY KEY E(R, RA)
ENCRYPTED SOFTWARE PROGRAM E(KB,SB)
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER E(RB,(KB,nB))
ENCRYPTED SUPPLEMENTARY KEY E(R, RB)
SOFTWARE PROGRAM SA
SOFTWARE PROGRAM SB
RECORDING MEDIUM 300
E(R,RA)
E(R', RA)
E(R, RB)
E(R', RB)
411
FOURTH DECRYPTING UNIT
RA, RB
R
RANDOM NUMBER STORING UNIT
401
R
R'
412
RANDOM NUMBER UPDATING UNIT
R'
413
SECOND ENCRYPTING UNIT
EXECUTING APPARATUS 400 (PART RELATING TO THE UPDATING OF THE ENCRYPTED SUPPLEMENTARY KEYS)

FIG. 3



0550022-042500

FIG. 4

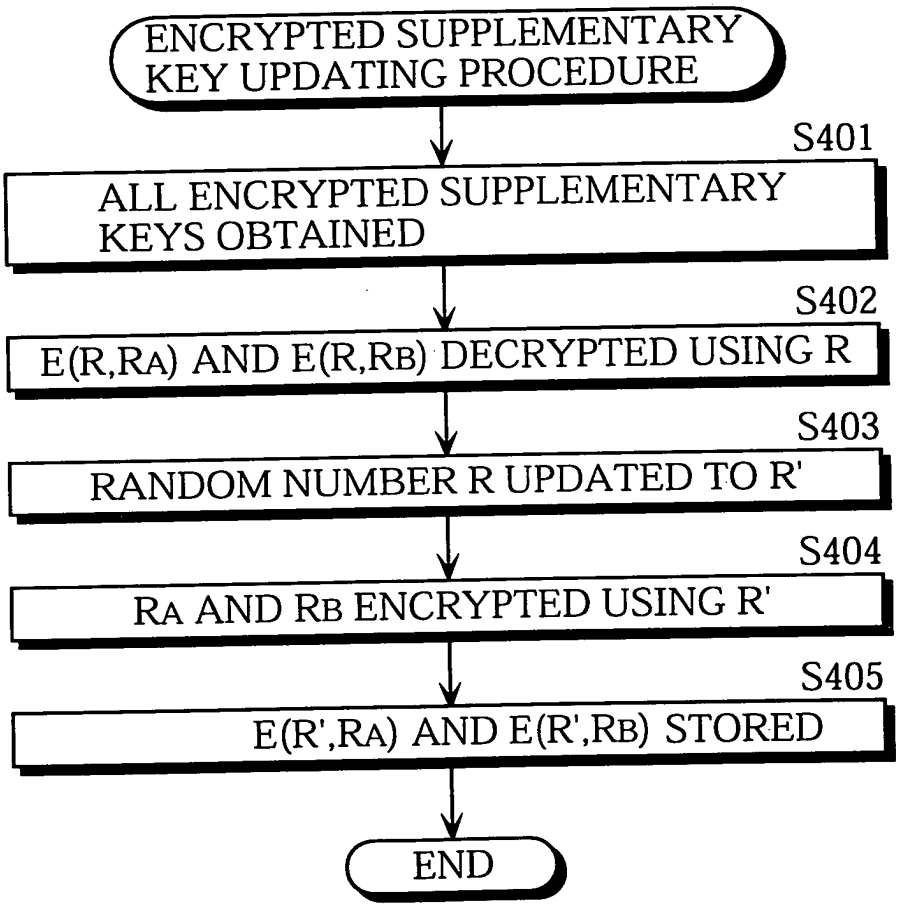

ENCRYPTED SUPPLEMENTARY KEY UPDATING PROCEDURE
S401
ALL ENCRYPTED SUPPLEMENTARY KEYS OBTAINED
S402
E(R,RA) AND E(R,RB) DECRYPTED USING R
S403
RANDOM NUMBER R UPDATED TO R'
S404
RA AND RB ENCRYPTED USING R'
S405
E(R',RA) AND E(R',RB) STORED
END

FIG. 5

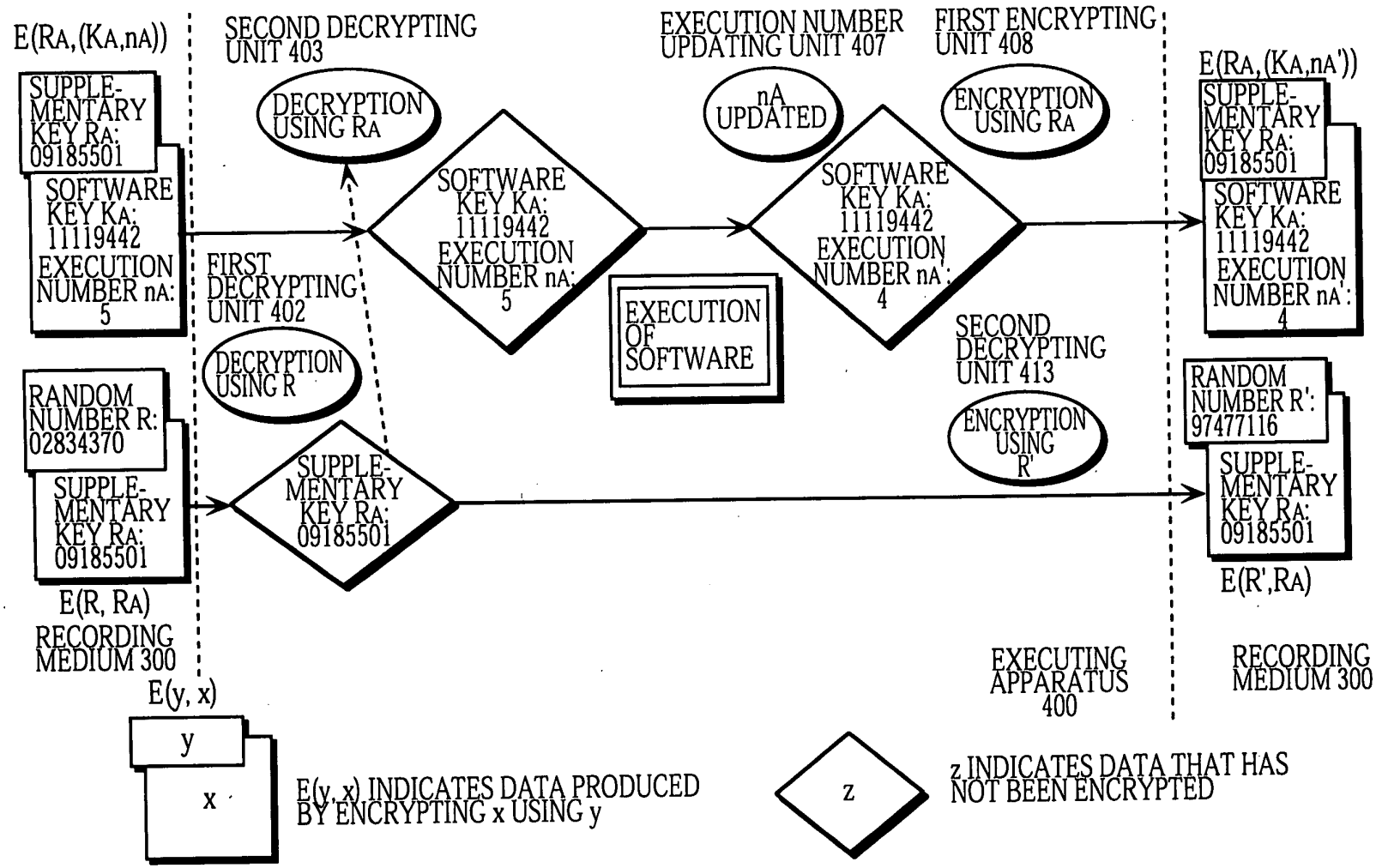

E(RA,(KA,nA))
SUPPLE-MENTARY KEY RA: 09185501
SOFTWARE KEY KA: 11119442 EXECUTION NUMBER nA: 5
RANDOM NUMBER R: 02834370
SUPPLE-MENTARY KEY RA: 09185501
E(R, RA)
RECORDING MEDIUM 300
SECOND DECRYPTING UNIT 403
DECRYPTION USING RA
FIRST DECRYPTING UNIT 402
DECRYPTION USING R
SOFTWARE KEY KA: 11119442 EXECUTION NUMBER nA: 5
SUPPLE-MENTARY KEY RA: 09185501
EXECUTION OF SOFTWARE
EXECUTION NUMBER UPDATING UNIT 407
nA UPDATED
SOFTWARE KEY KA: 11119442 EXECUTION NUMBER nA: 4
FIRST ENCRYPTING UNIT 408
ENCRYPTION USING RA
SECOND DECRYPTING UNIT 413
ENCRYPTION USING R'
E(RA,(KA,nA'))
SUPPLE-MENTARY KEY RA: 09185501
SOFTWARE KEY KA: 11119442 EXECUTION NUMBER nA': 4
RANDOM NUMBER R': 97477116
SUPPLE-MENTARY KEY RA: 09185501
E(R',RA)
EXECUTING APPARATUS 400
RECORDING MEDIUM 300
E(y, x)
y
x
E(y, x) INDICATES DATA PRODUCED BY ENCRYPTING x USING y
z
z INDICATES DATA THAT HAS NOT BEEN ENCRYPTED

FIG. 6

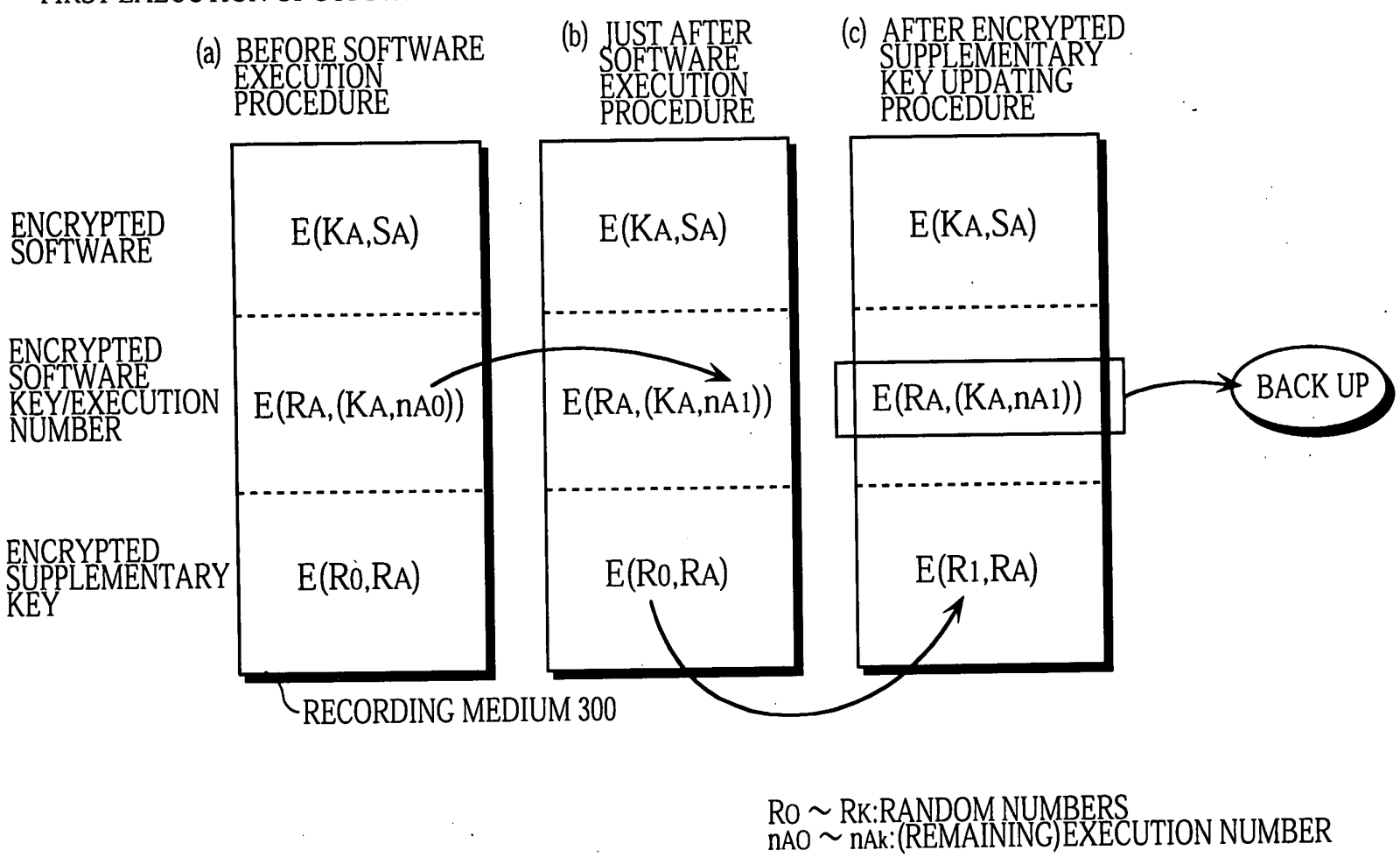

FIRST EXECUTION OF SOFTWARE PROGRAM SA
(a) BEFORE SOFTWARE EXECUTION PROCEDURE
(b) JUST AFTER SOFTWARE EXECUTION PROCEDURE
(c) AFTER ENCRYPTED SUPPLEMENTARY KEY UPDATING PROCEDURE
ENCRYPTED SOFTWARE
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER
ENCRYPTED SUPPLEMENTARY KEY
E(KA,SA)
E(KA,SA)
E(KA,SA)
E(RA,(KA,nA0))
E(RA,(KA,nA1))
E(RA,(KA,nA1))
BACK UP
E(R0,RA)
E(R0,RA)
E(R1,RA)
RECORDING MEDIUM 300
R0 ~ RK:RANDOM NUMBERS
nA0 ~ nAk:(REMAINING)EXECUTION NUMBER

FIG. 7

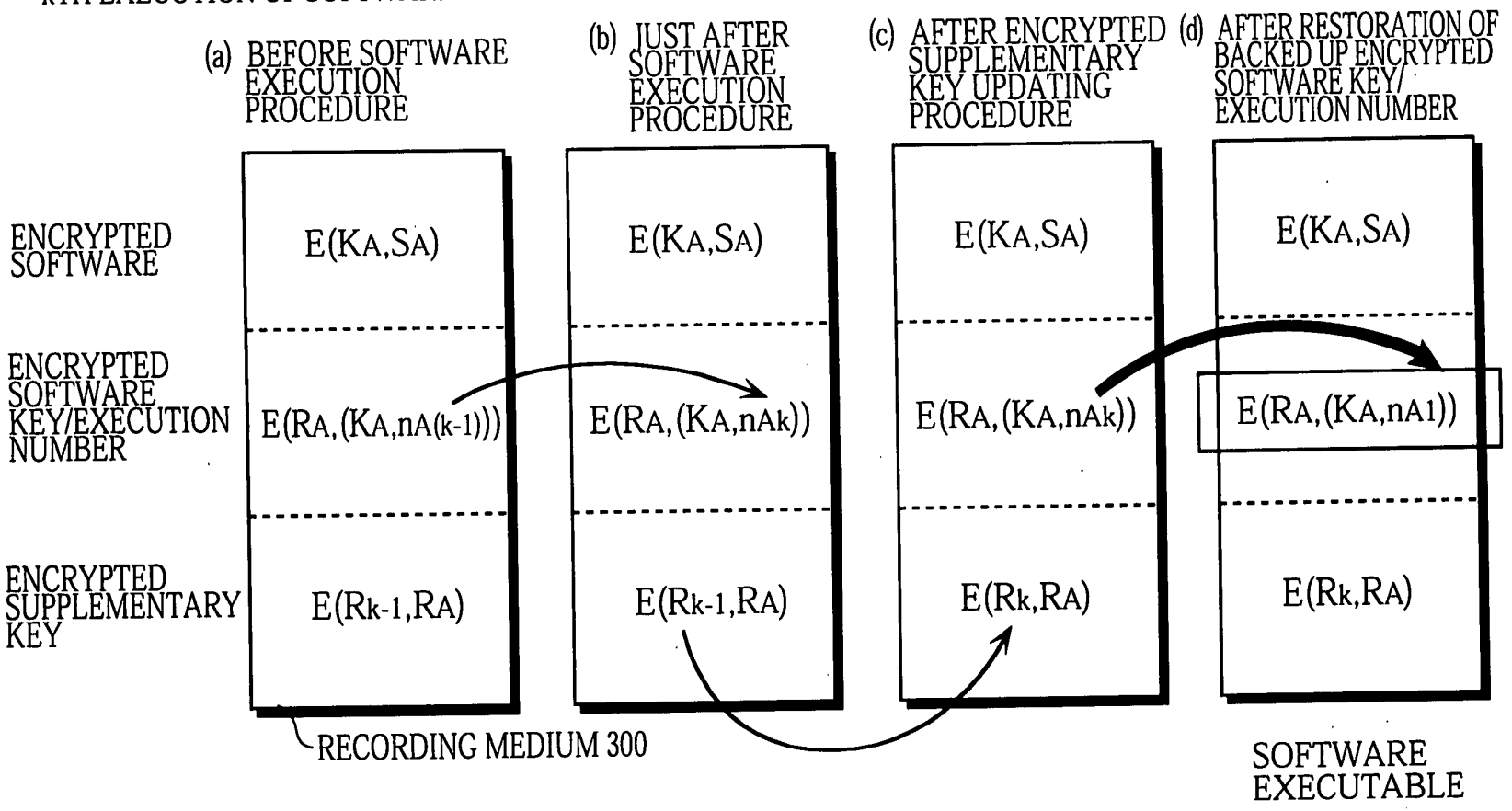

kTH EXECUTION OF SOFTWARE PROGRAM SA
(a) BEFORE SOFTWARE EXECUTION PROCEDURE
(b) JUST AFTER SOFTWARE EXECUTION PROCEDURE
(c) AFTER ENCRYPTED SUPPLEMENTARY KEY UPDATING PROCEDURE
(d) AFTER RESTORATION OF BACKED UP ENCRYPTED SOFTWARE KEY/ EXECUTION NUMBER
ENCRYPTED SOFTWARE
ENCRYPTED SOFTWARE KEY/EXECUTION NUMBER
ENCRYPTED SUPPLEMENTARY KEY
E(KA,SA)
E(RA,(KA,nA(k-1)))
E(Rk-1,RA)
E(KA,SA)
E(RA,(KA,nAk))
E(Rk-1,RA)
E(KA,SA)
E(RA,(KA,nAk))
E(Rk,RA)
E(KA,SA)
E(RA,(KA,nA1))
E(Rk,RA)
RECORDING MEDIUM 300
SOFTWARE EXECUTABLE

FIG. 8

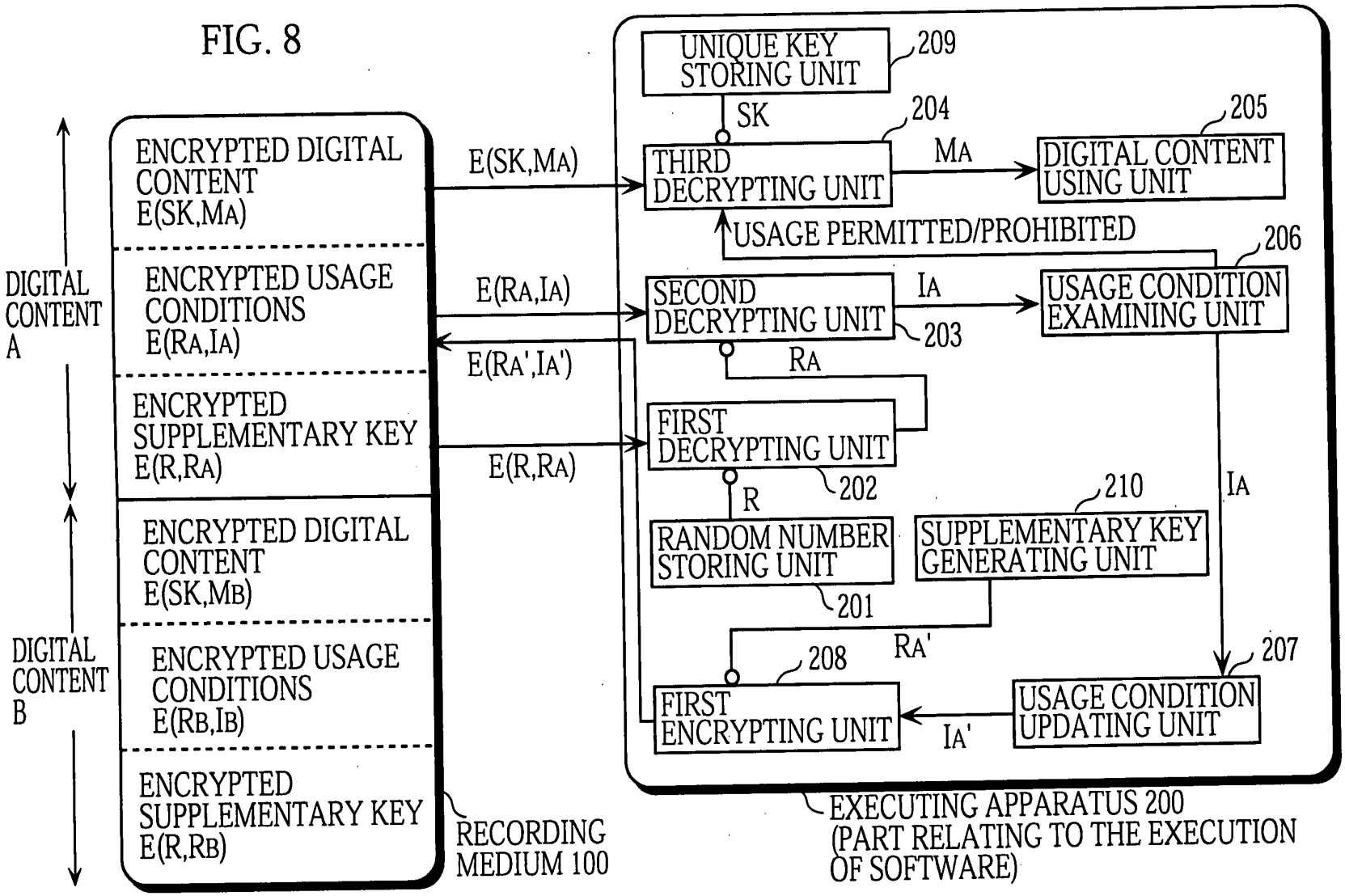

DIGITAL CONTENT A
DIGITAL CONTENT B
ENCRYPTED DIGITAL CONTENT E(SK,MA)
ENCRYPTED USAGE CONDITIONS E(RA,IA)
ENCRYPTED SUPPLEMENTARY KEY E(R,RA)
ENCRYPTED DIGITAL CONTENT E(SK,MB)
ENCRYPTED USAGE CONDITIONS E(RB,IB)
ENCRYPTED SUPPLEMENTARY KEY E(R,RB)
RECORDING MEDIUM 100
E(SK,MA)
E(RA,IA)
E(RA',IA')
E(R,RA)
UNIQUE KEY STORING UNIT
209
SK
THIRD DECRYPTING UNIT
204
MA
DIGITAL CONTENT USING UNIT
205
USAGE PERMITTED/PROHIBITED
206
SECOND DECRYPTING UNIT
IA
203
USAGE CONDITION EXAMINING UNIT
RA
FIRST DECRYPTING UNIT
202
R
RANDOM NUMBER STORING UNIT
201
210
SUPPLEMENTARY KEY GENERATING UNIT
IA
RA'
208
207
FIRST ENCRYPTING UNIT
IA'
USAGE CONDITION UPDATING UNIT
EXECUTING APPARATUS 200 (PART RELATING TO THE EXECUTION OF SOFTWARE)

FIG. 9

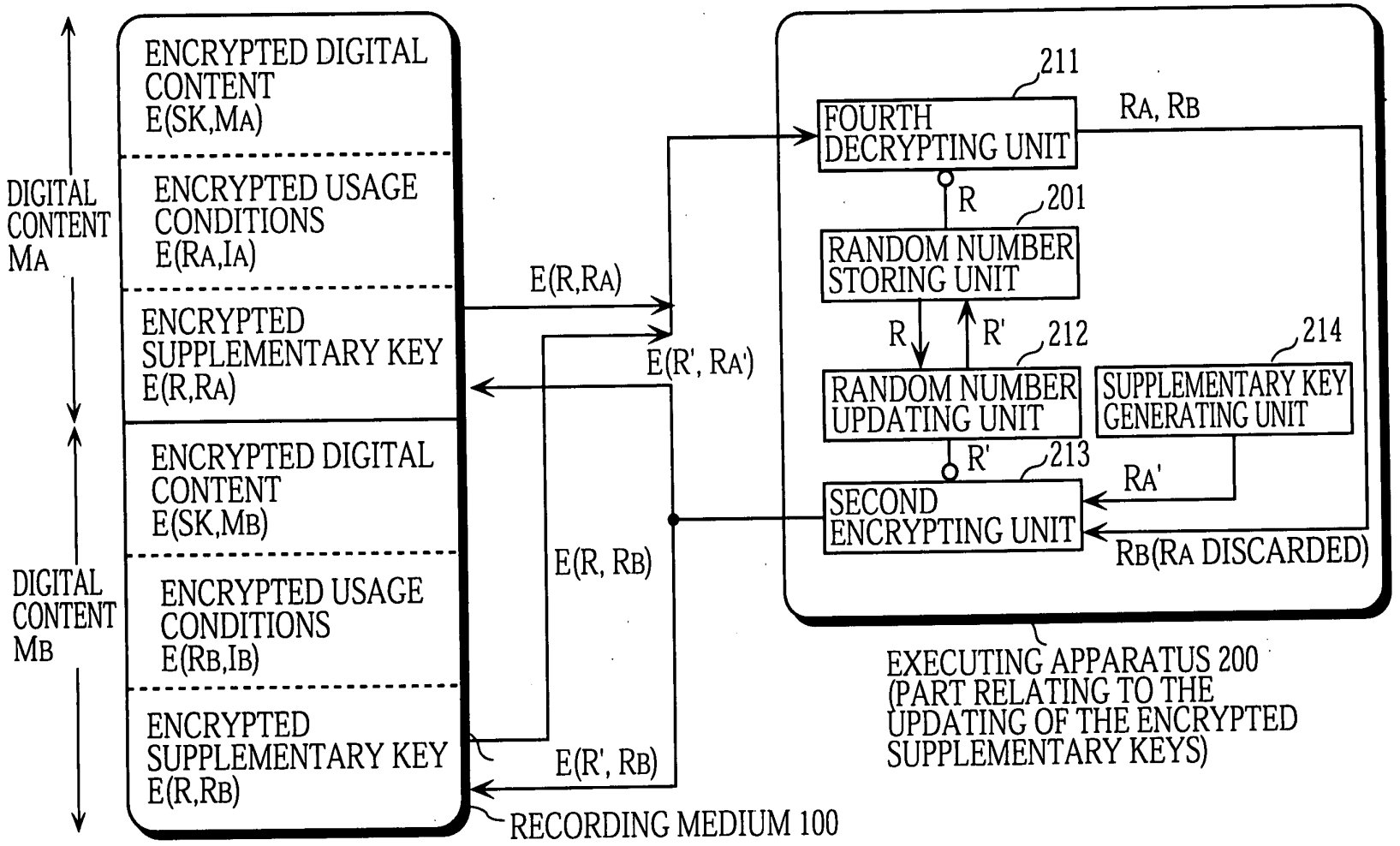

DIGITAL CONTENT MA
DIGITAL CONTENT MB
ENCRYPTED DIGITAL CONTENT E(SK,MA)
ENCRYPTED USAGE CONDITIONS E(RA,IA)
ENCRYPTED SUPPLEMENTARY KEY E(R,RA)
ENCRYPTED DIGITAL CONTENT E(SK,MB)
ENCRYPTED USAGE CONDITIONS E(RB,IB)
ENCRYPTED SUPPLEMENTARY KEY E(R,RB)
RECORDING MEDIUM 100
E(R,RA)
E(R', RA')
E(R, RB)
E(R', RB)
211
FOURTH DECRYPTING UNIT
RA, RB
R
201
RANDOM NUMBER STORING UNIT
R
R'
212
214
RANDOM NUMBER UPDATING UNIT
SUPPLEMENTARY KEY GENERATING UNIT
R'
213
RA'
SECOND ENCRYPTING UNIT
RB(RA DISCARDED)
EXECUTING APPARATUS 200 (PART RELATING TO THE UPDATING OF THE ENCRYPTED SUPPLEMENTARY KEYS)

FIG. 10

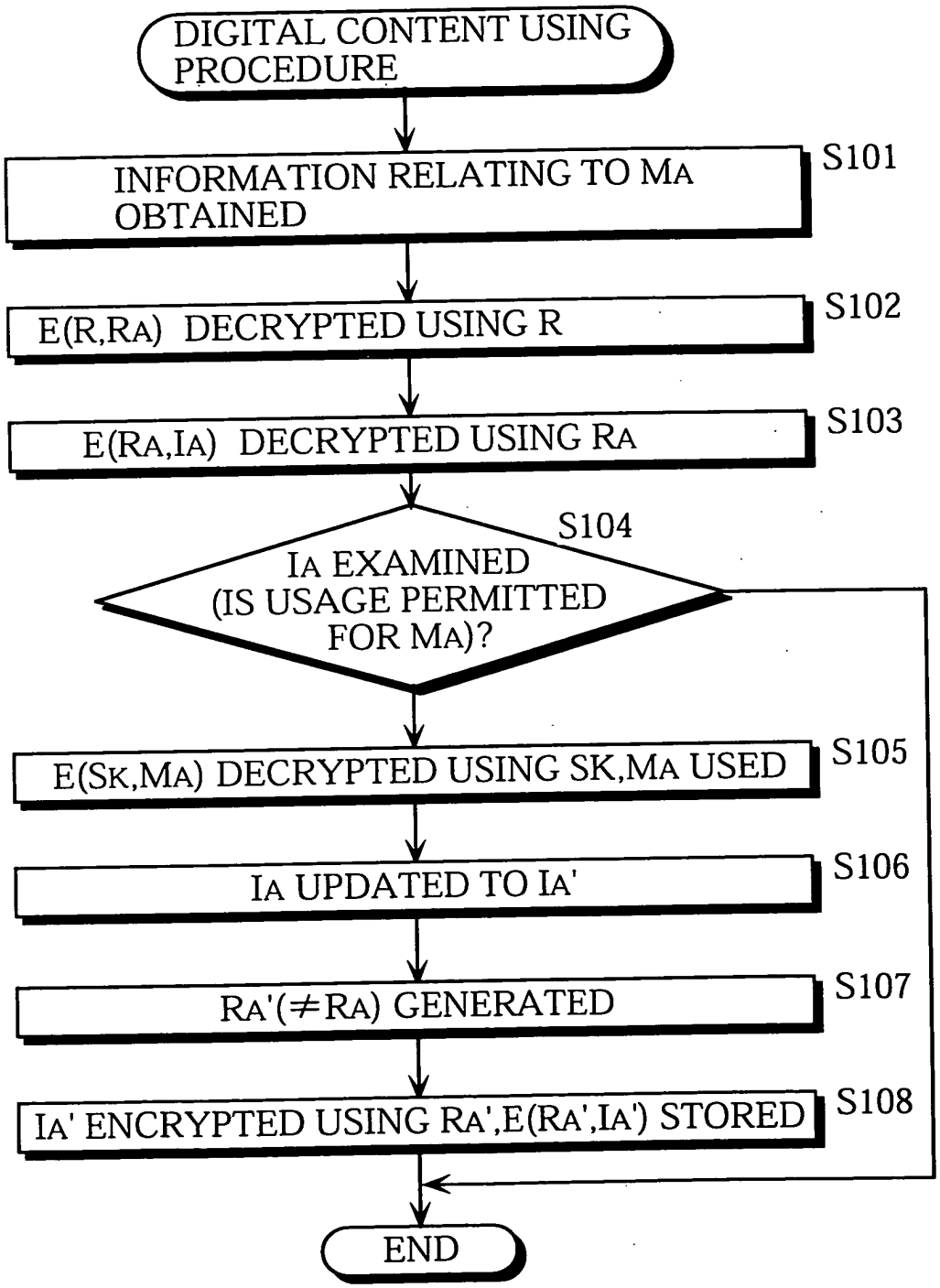
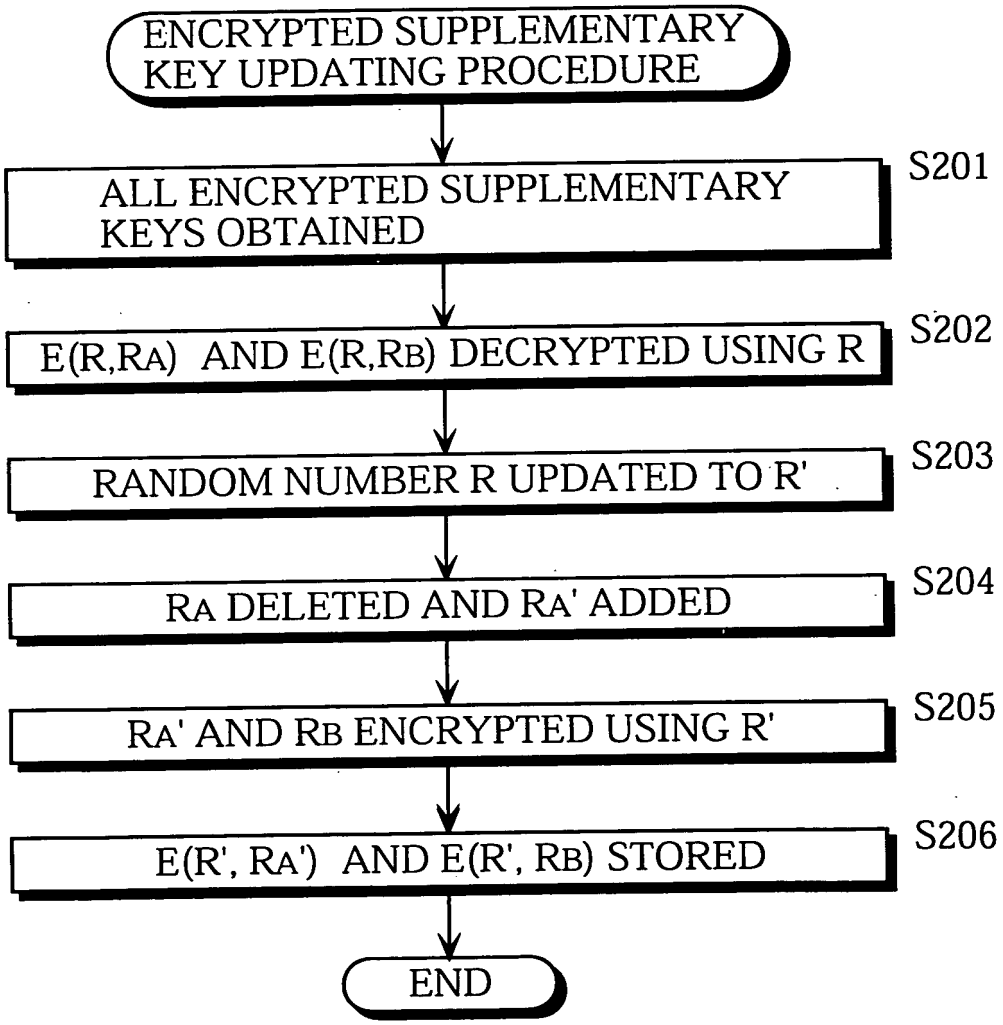

DIGITAL CONTENT USING PROCEDURE
INFORMATION RELATING TO MA OBTAINED
S101
E(R,RA) DECRYPTED USING R
S102
E(RA,IA) DECRYPTED USING RA
S103
IA EXAMINED (IS USAGE PERMITTED FOR MA)?
S104
E(SK,MA) DECRYPTED USING SK,MA USED
S105
IA UPDATED TO IA'
S106
RA'(≠RA) GENERATED
S107
IA' ENCRYPTED USING RA',E(RA',IA') STORED
S108
END

FIG. 11



0955802 - 042506

FIG. 12

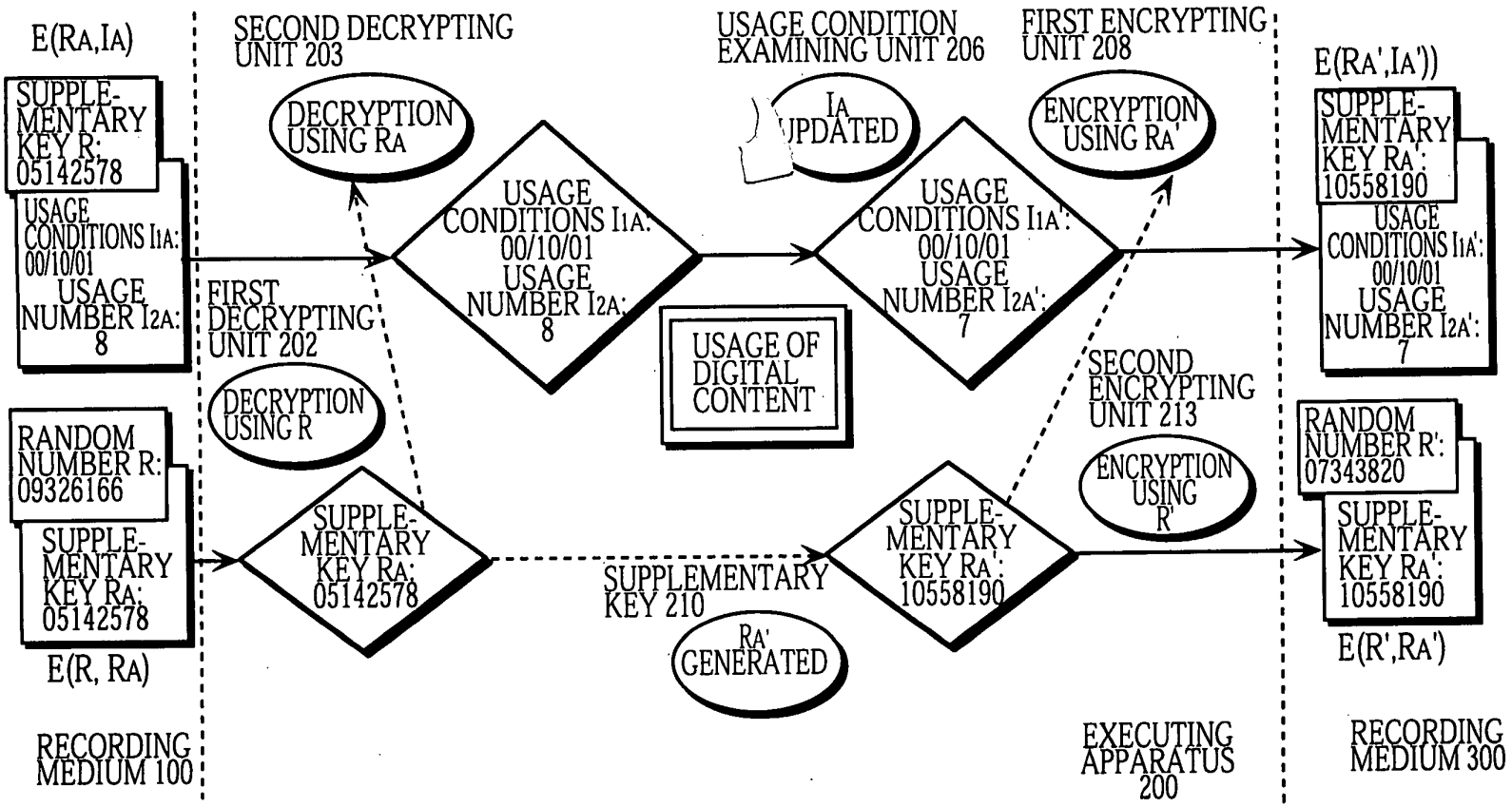

E(RA,IA)
SUPPLE-MENTARY KEY R: 05142578
USAGE CONDITIONS I1A: 00/10/01 USAGE NUMBER I2A: 8
RANDOM NUMBER R: 09326166
SUPPLE-MENTARY KEY RA: 05142578
E(R, RA)
RECORDING MEDIUM 100
SECOND DECRYPTING UNIT 203
DECRYPTION USING RA
FIRST DECRYPTING UNIT 202
DECRYPTION USING R
SUPPLE-MENTARY KEY RA: 05142578
USAGE CONDITIONS I1A: 00/10/01 USAGE NUMBER I2A: 8
USAGE CONDITION EXAMINING UNIT 206
IA UPDATED
USAGE OF DIGITAL CONTENT
USAGE CONDITIONS I1A': 00/10/01 USAGE NUMBER I2A': 7
SUPPLEMENTARY KEY 210
RA' GENERATED
SUPPLE-MENTARY KEY RA': 10558190
FIRST ENCRYPTING UNIT 208
ENCRYPTION USING RA'
SECOND ENCRYPTING UNIT 213
ENCRYPTION USING R'
EXECUTING APPARATUS 200
E(RA',IA'))
SUPPLE-MENTARY KEY RA': 10558190
USAGE CONDITIONS I1A': 00/10/01 USAGE NUMBER I2A': 7
RANDOM NUMBER R': 07343820
SUPPLE-MENTARY KEY RA': 10558190
E(R',RA')
RECORDING MEDIUM 300

FIG. 13

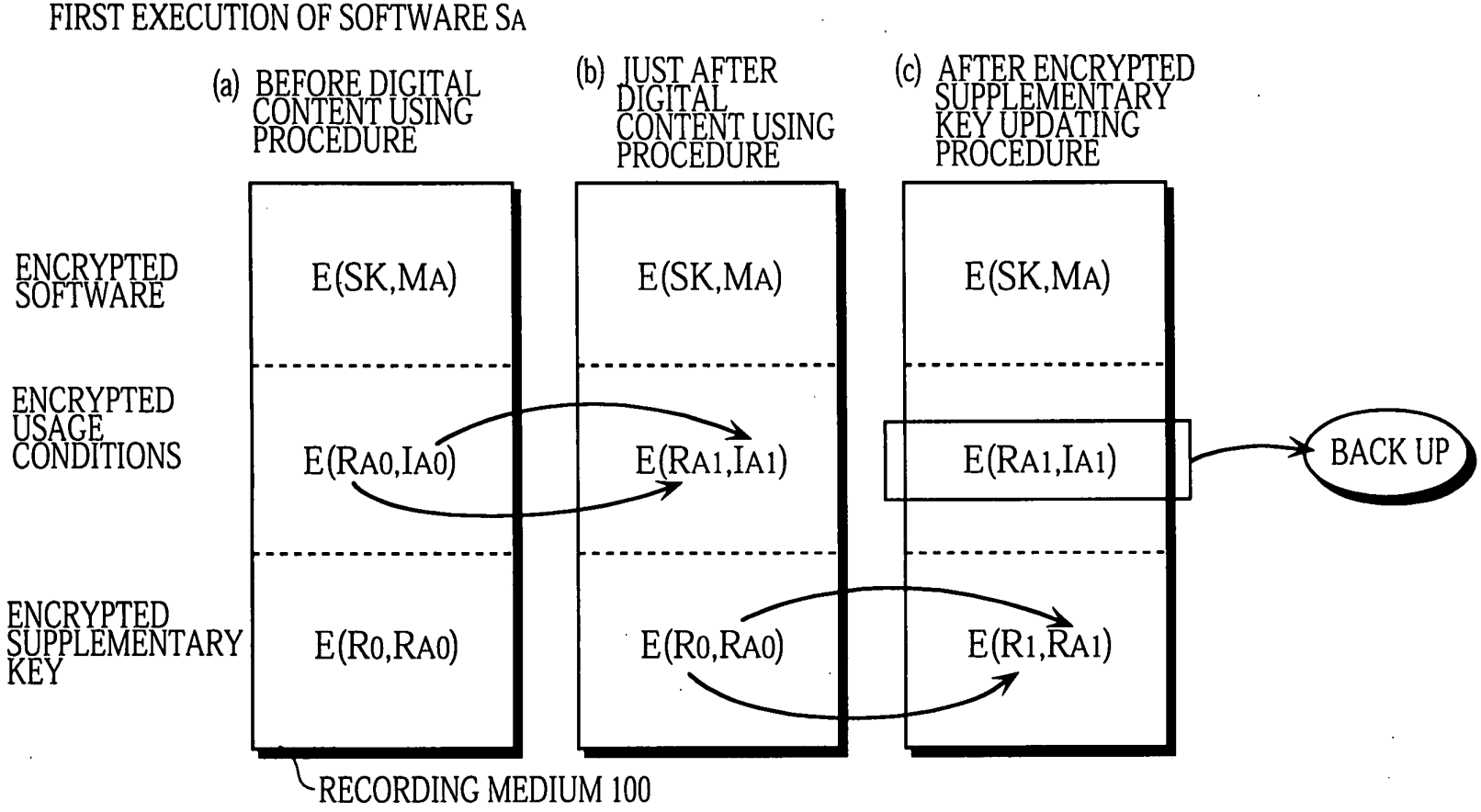
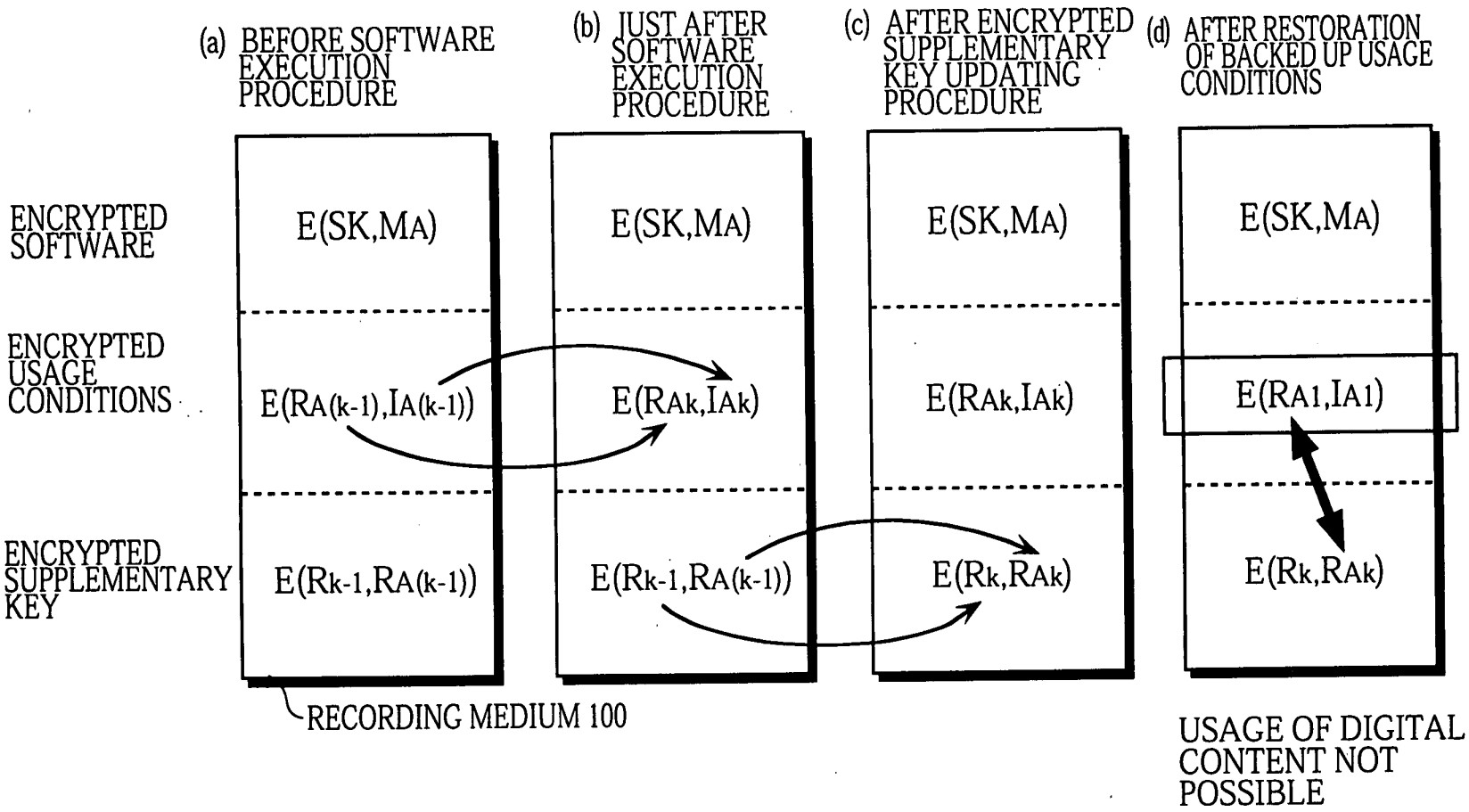

FIRST EXECUTION OF SOFTWARE SA
(a) BEFORE DIGITAL CONTENT USING PROCEDURE
(b) JUST AFTER DIGITAL CONTENT USING PROCEDURE
(c) AFTER ENCRYPTED SUPPLEMENTARY KEY UPDATING PROCEDURE
ENCRYPTED SOFTWARE
ENCRYPTED USAGE CONDITIONS
ENCRYPTED SUPPLEMENTARY KEY
E(SK,MA)
E(SK,MA)
E(SK,MA)
E(RA0,IA0)
E(RA1,IA1)
E(RA1,IA1)
BACK UP
E(R0,RA0)
E(R0,RA0)
E(R1,RA1)
RECORDING MEDIUM 100

FIG. 14


kTH EXECUTION OF SOFTWARE PROGRAM SA
(a) BEFORE SOFTWARE EXECUTION PROCEDURE
(b) JUST AFTER SOFTWARE EXECUTION PROCEDURE
(c) AFTER ENCRYPTED SUPPLEMENTARY KEY UPDATING PROCEDURE
(d) AFTER RESTORATION OF BACKED UP USAGE CONDITIONS
ENCRYPTED SOFTWARE
ENCRYPTED USAGE CONDITIONS
ENCRYPTED SUPPLEMENTARY KEY
E(SK,MA)
E(RA(k-1),IA(k-1))
E(Rk-1,RA(k-1))
E(RAk,IAk)
E(Rk,RAk)
E(RA1,IA1)
RECORDING MEDIUM 100
USAGE OF DIGITAL CONTENT NOT POSSIBLE